Detection of Sybil Attacks in Participatory Sensing using Cloud based Trust Management System

Shih-Hao Chang
Department of Computer Science and Information Engineering
Tamkang University
New Taipei City, Taiwan
sh.chang@ieee.org

Yeong-Sheng Chen
Department of Computer Science
National Taipei University of Education
Taipei City, Taiwan
yschen@tea.ntue.edu.tw

Shin-Ming Cheng
Department of Computer Science and Information Engineering
National Taiwan University of Science and Technology
Taipei City, Taiwan
smcheng@mail.ntust.edu.tw

***Abstract*—Participatory sensing is a revolutionary paradigm in which volunteers collect and share information from their local environment using mobile phones. Different from other participatory sensing application challenges who consider user privacy and data trustworthiness, we consider network trustworthiness problem namely Sybil attacks in participatory sensing. Sybil attacks focus on creating multiple online user identities called Sybil identities and try to achieve malicious results through these identities. In this paper, we proposed a Cloud based Trust Management Scheme (CbTMS) framework for detecting Sybil attacks in participatory sensing network. Our CbTMS was proposed for performing Sybil attack characteristic check and trustworthiness management system to verify coverage nodes in the participatory sensing. To verify the proposed framework, we are currently developing the proposed scheme on OMNeT++ network simulator in multiple scenarios to achieve Sybil identities detection in our simulation environment.**

I. Introduction

In recent years, huge growth in mobile computing devices such as smartphones and tablet computers on the market make people's life more convenient. Different from last century, the mobile phone of today, namely smartphone, have usually come with multiple embedded sensors, such as camera, microphone, GPS, accelerometer, digital compass and gyroscope. These technologies empowered smartphone users to collect data from their surrounding environment and upload them to an application server using existing communication infrastructure (e.g., 3G service or WiFi access points). Smartphones provide an excellent platform for participatory sensing application [1]. Hence, a requester of data can create tasks that uses the general public to capture geo-tagged images, videos, or audio snippets. Participants who have installed the client APPs on their smart phones can submit their data and get rewarded. For example, Panoramic 3-D photosynthesis of businesses and restaurants photos from Gigwalk has been collected by Microsoft Bing Map.

A profusion of novel and exciting participatory sensing applications have emerged that ranging from health care to multiple cultural aspects over the past few years. Two examples of participatory sensing applications are BALANCE [2] and HealthSense [3] are used to collect and share data about personal health projects which monitor the activities and behavior of their diet, and encourage healthy living. Participatory sensing provides a very openness which allows anyone to contribute data, however, also exposes the applications to malicious and erroneous attack. Sharing sensed data tagged with spatial-temporal information could reveal a lot of personal information, such as user's identity, personal activities, political views, health status, etc., which poses threats to the participating users. Malicious participants may inadvertently position the phone in an undesirable position or deliberately contribute bad data while collecting sensor readings.

There have been plenty of research efforts that have investigated privacy techniques for anonymous data collection in location based services (LBS) and particularly in participatory sensing systems. Most of the current researches in participatory sensing have focused on user privacy and anonymity [4], [5], with little work on network integrity and protection. However, mobile phone in telecommunication network rely on assumptions of identity, where each mobile phone's IMEI (International Mobile Equipment Identity) numbers represents one identity. Hence, an attacker with many identities can use them to act maliciously, by either stealing information or provide incorrect data in participatory sensing environment, namely Sybil Attack. The Sybil attack was first introduced by Microsoft researcher J. R. Douceur [6]. A Sybil attack relies on the fact that a participatory sensing network data server cannot ensure that each unknown data collecting element is a distinct, mobile phone. Therefore, any malicious participatory sensing network attack can try to inject false information into the network to confuse or even collapse the network applications.

Cloud computing has been receiving much attention as a new computing paradigm for providing flexible and on-demand infrastructures. Everything is treated as a service (i.e. XaaS), e.g. SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) and these services define a layered system structure for cloud computing. However, trust management is one of the most challenging issues in the emerging cloud computing. Although many approaches have been proposed recently for trust management in cloud environments, not much attention has been given to determining the credibility of trust feedbacks. To solve this problem, we propose a Cloud based Trust Management System (CbTMS) framework for evaluating the trustworthiness

of volunteer networks in participatory sensing applications. Our TMS framework allows a credit calculator associate with mobile devices that reflects the level of trust perceived over a period of time. A high credit score is an indication that a particular mobile device has been reporting reliable communication in the past. To verify our idea, we utilizing OMNeT++ simulation to show its effectiveness against Sybil attacks.

The rest of this paper is organized as follows. Section II presents related works and summarized. Section III provides the detection factors to motivate the need for a reputation system in the context of participatory sensing and presents an overview of the system architecture respectively. In Section IV, we describe the experimental setup. Section V concludes the paper.

II. Background

In recent years, more and more participatory sensing applications apply in different fields. For example, in personal health monitoring, BALANCE [2] provides allows the client to monitor the activities and behavior of their diet, and encourage healthy living. It is the use of mobile phones enters the food calories and accelerator detects movement patterns and time to project the calories consumed to achieve health management. HealthSense [3] automatically detect health-related events, such as pain or depression cannot be observed directly through the current sensor technology. HealthSense analyze sensor data from the patient by machine learning techniques. The system uses patient input events to assist in classification (such as pain or itching). Finally, user provides feedback to the machine learning process. As mentioned, participatory sensing applications are exposes the applications to malicious an erroneous attacks.

The first Sybil attack was described by Douceur in the context of peer-to-peer networks [6]. He showed that there is no practical solution for this attack and pointed out that it could defeat the redundancy mechanisms of distributed storage systems. Problems arise when a reputation system (such as a trusted certification) is tricked into thinking that an attacking computer has a disproportionally large influence. Grover [7] proposed a scheme to protect against the Sybil attack using neighboring nodes information. In this approach every node participate to detect the suspect node in the network. Every mobile node have different group of neighbors at different time interval. After sharing their tables they match their neighboring table, if some nodes are simultaneously observed with same set of neighbors at different interval of time, then these node are under Sybil attack. In this case, identities are neighboring nodes that associated to specific trust devices. Similar to a central authority creating certificates, there are few ways to prevent an attacker from attaining multiple devices.

The concepts of trust and reputation have been shown to be promising concepts to support the customers in such situations in selecting a high quality service [8]. Trust and reputation are similar concepts and in computational models both are often based on history of past interactions.However, building up trust and reputation usually requires long-term identifiers which can be link over numerous transactions. At a first glance, this seems to be in conflict with the protection of the user's privacy, as unlinkability is a key term when referring to privacy properties. To solve this problem, Bayesian trust models [9] naturally allow for the interpretation of trust as a subjective probability, which allows for the consideration of personal preferences and context-dependent parameters. However, building up trust and reputation usually requires long-term identifiers which can be link over numerous transactions.

Trust management is one of the critical issues in cloud computing and a very active research area [10], [11]. Brandic *et al.* Over the past few years, many studies have proposed different techniques to address trust management issues. For instance, [10] proposed a centralized approach in cloud environments using compliant management to help the cloud service consumers to support the cloud service consumer's perspective in selecting proper cloud services. Unlike previous works that use centralized architecture, they present a credibility model supporting distributed trust feedback assessment and storage. This credibility model also distinguishes between trustworthy and malicious trust feedback. Hwang *et al.* [11] proposed a security aware cloud architecture where trust negotiation and data coloring techniques are used to support the cloud service provider perspective. The cloud service consumer's perspective is supported using the trust-overlay networks to deploy a reputation-based trust management.

Due to in the participatory sensing applications, participants allowed anyone with an appropriate device that gets the application installed to a register as a participant. Such kind of human intervention entail serious security and privacy risks. Human behavior will involve additional security challenges. User's sensor data unboundedly transmit could results in leak of privacy. For instance, user may leak his/her personal identity information by nature of personal response. Due to user may receive incorrect data from network that will lead integrity problem as it comes from malicious participants. For example, the malicious user can tamper and report data to other participants [4]. However, in the participatory sensing, introduces different security issues because devices are already in the hands of potential adversaries. A misbehaving participant may produce false sensing data or send false data randomly with certain probability to deceive the server [5].

In this section, we overview the state of art projects that design and the implementation of the participatory sensing, cloud computing framework and trust models. However, their approaches are not applicable to detect Sybil attacks in participatory sensing environments by utilize trust management system. Therefore, we attempt to identify Sybil attacks in participatory sensing environment by utilizing a Cloud based Trust Management System that distinguish between credible trust nodes' feedbacks and malicious trust nodes' feedbacks through a credibility model.

III. Detection the Sybil Attack in Participatory Sensing Factors

We refer to the participants, i.e., smartphone users, in the system as entities. Interactions are actions between entities, i.e., the usage of a service or a capability that is offered by a service provider, e.g., buying goods or information. Hence, the type of interaction specifies the service context, in which a smartphone user, namely entity A, wants to interact with a service provider. Whenever, an entity A is in the role of the initiator of an interaction, i.e., entity A has to select a service provider from a set of available service providers, it may evaluate the trustworthiness of the available service providers a basis for the selection. Hereby, entity A uses its direct evidence from previous interactions and recommendations (also called indirect evidence). Having collected direct evidence and recommendations about one or multiple service providers, the trust model can be used for aggregating the evidence removing or giving lower weight to recommendations from unreliable sources and deriving trust values for the service providers, which then can be the basis for the decision whether to interact with one of the available service providers at all, and which service provider to select.

We propose a cloud based service management framework implemented in a service provider using the Service Oriented Architecture (SOA) to deliver trust as a service. SOA and Web services are one of the most important enabling technologies for cloud computing in the sense that resources (e.g., software, infrastructures, and platforms) are exposed in clouds as services. In particular, our framework uses Web services to interact with several distributed smartphone nodes that expose interfaces so that trust participants (other smartphone nodes) can give their trust feedbacks or inquire about the trust results based on feedback messages. Fig. 1, depicts the framework, which consists of three different layers, namely the Cloud Service Provider Layer, the Trust Management System Layer, and the Cloud Service Consumer Layer.

- The Cloud Service Provider Layer consists of different cloud service providers who provide cloud services. The minimum indicative feature that every cloud service provider should have is to provide the infrastructure as a service (i.e., the cloud provider should have a data center that provides the storage, the process, and the communication).
- The Trust Management System Layer. This layer consists of several distributed Trust Management System (TMS) nodes that expose interfaces so that cloud service consumers can give their trust feedbacks or inquire about the trust results represents.
- The Cloud Service Consumer Layer. Finally, this layer consists of different cloud service consumers who consume cloud services. For example, a new startup that has limited funding can consume cloud services (e.g., hosting their services in Amazon S3). A cloud service consumer can give trust feedbacks of a particular cloud service by invoking the TMS.

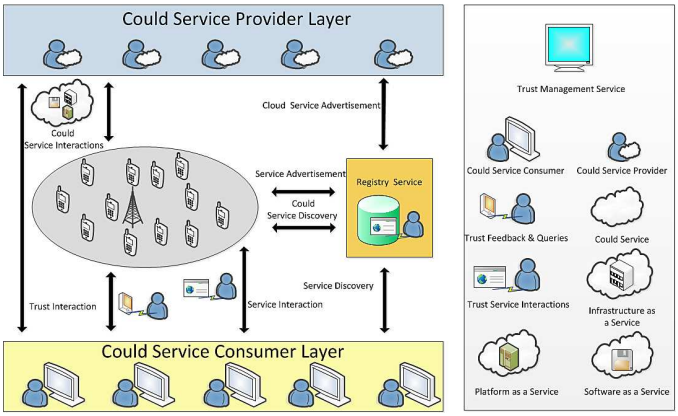

Fig. 1. Architecture of the Trust as a Service Framework

As mentioned, participatory sensing nodes are exposed to malicious participants may deliberately contribute forge nodes and bad data. These malicious participants also can exploit these links to de-anonymize the volunteers and compromise their privacy. Like other networks, the security requirements in participatory sensing include services such as authentication, confidentiality, integrity, and access control such as Sybil attack and slandering should be addressed. Once the Sybil attack participatory sensing, a Sybil node impersonating multiple identities has an important feature that can be detected by knowing the characteristics. For example, all the identities are part of the same physical device, they must move in unity way, while independent nodes are free to move at will. As nodes move geographically, all the Sybil identities will appear or disappear simultaneously as the attacker moves in and out of range.

We develop this CbTMS to exploit Sybil attack characteristics to perform Sybil attack detection based on the following two assumptions:

- First, we assume that each user and service provider who wants to participate in the system owns a unique, initial identifier, which is obtained at the bootstrapping phase from a party that is trusted by all involved parties (i.e., users, service directory provider, and service providers).
- Second, we assume the Sybil nodes uses a single-channel radio, multiple Sybil nodes must transmit serially, whereas multiple independent nodes can transmit in parallel.

1) Characteristics Checking Scheme: This CbTMS framework include a passive Characteristics Checking Schemes (CCS) that keep Sybil nodes in check including time, density and topology in the simultaneously. The idea of this CCS introduces an adaptive threshold (similar as the watchdog implementation method) to detect the characteristics of a Sybil attacks in participatory sensing network. This CCS will be implemented in the cloud-side which regularly check the coverage participatory sensing nodes condition to decide whether the node either genuine identity or has been compromised. The CCS will set multiple adaptive thresholds to monitor covered

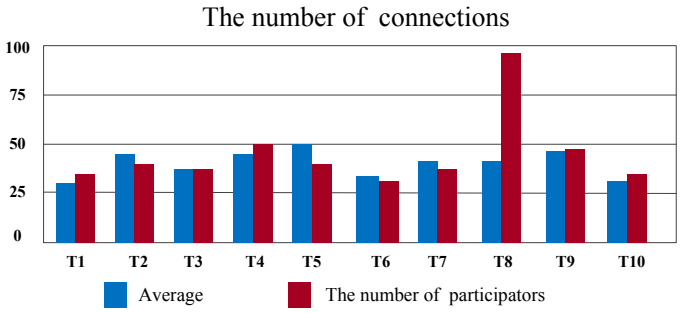

Fig. 2. A diagram of suspicious Sybil attacks activities for a short period of time

participatory sensing nodes' characteristics and implemented as part of the system operation process running on the cloud server. When a requester inquire trust credit to a inspector from CbTMS framework, if the passive CCS does not detect any attack pattern on the node, it returns no attack pattern found to requester. Otherwise, it will notify requester to disconnect suspicious malicious node(s).

2) Time: Once a Sybil node has compromising a partial participatory sensing, its will create a number of online identities and use these identities to compromise participate sensing. Hence, in utilizing server statistics number of connected participants for a brief period of time, we can first distinguish between suspect Sybil attacks in participatory sensing network. By analyzing this statistics, we can infer system whether has suspicious Sybil nodes at that time period. We assume current number of connected participatory is S_c, statistics number of connected participatory at this time is S_r, and set threshold ϵ. Detective method is defined as follows.

$$\frac{S_c}{S_r} = \begin{cases} \text{It could has some dubitable node,} & \text{if } \frac{S_c}{S_r} > \epsilon, \\ \text{It could has no any dubitable node,} & \text{if } \frac{S_c}{S_r} \leq \epsilon. \end{cases} \quad (1)$$

As shown in Fig. 2, we assume this system's threshold ϵ is 2 with S_c and S_r are 100 and 40 at T8. As presented in (1), we can know while S_c divided by S_r is greater than ϵ. In this situation, the system can assume the suspected Sybil nodes existed in participatory sensing network.

3) Density: Moreover, after filtered the time factor to monitor suspected Sybil identities, our passive detection scheme will based on the fundamental assumption that the probability of two mobile users having exactly the same set of neighbors in a sub-region and its topographical map will smaller than 1000m x 1000m [12]. Each sub-region usually has regular density, hence we can exploit this characteristic to detect suspected Sybil nodes. Using server statistic each region's density for a brief period of time. We assume each sub-region is inside a base station coverage range. By this statistics report, we can infer system whether has suspected Sybil node in his sub-region. we assume current region's density is D_c, statistics region's density is D_r, and set threshold θ. Detective method is defined as follows.

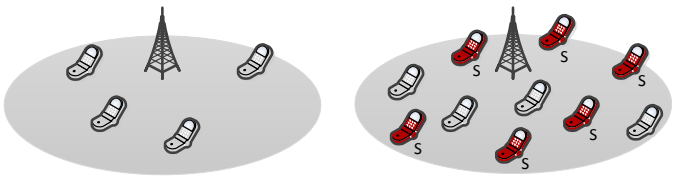

Fig. 3. A diagram of suspicious Sybil attacks activities in a region

$$\frac{D_c}{D_r} = \begin{cases} \text{It could has some dubitable node,} & \text{if } \frac{D_c}{D_r} > \theta, \\ \text{It could has no any dubitable node,} & \text{if } \frac{D_c}{D_r} \leq \theta. \end{cases} \quad (2)$$

As shown in Fig. 3, left is statistics sub-region's density and right is current sub-region's density. Nodes that has a mark "S" are a suspected Sybil identities, so we can observe current sub-region's density is greater than statistics sub-region's density in a brief period of time. In this situation, the system can assume the suspected Sybil nodes existed in participatory sensing network.

4) Network Topology: Due to each Sybil group will present a similar topography map, nodes will be very frequently heard together even when they are not Sybil identities and will rarely be heard apart as they do not move out of radio range. This leads to the false identification rate in topographies that are denser in terms of nodes per square meter. Hence, the accuracy and error rates for a single node observer when a Sybil attacker present will be very obvious. Again, in smaller topographies there is insufficient mixing to separate Sybil identities from real nodes, and the error rate is high, as is the detection rate, because all nodes are seen as part of the same identity. As the topography size increases, the number of meaningful observations that a single node can make increases, and the true positive rate stays high, on the order of 95%, while the false positive rate drops significantly. As the topography size increases further, the number of observations that a single node can make is reduced as all nodes are spread far apart, and the accuracy of identifying the Sybil identities decreases.

As shown in Fig. 4, when Sybil attacks is present, the network topology can be conceptually divided into two parts: one consisting of all genuine identities and the other consisting of all Sybil identities. The link connecting a genuine node to a Sybil node is called an attack edge [13].

5) Trust Credit Assessment: In our framework, the trust credit of a participatory sensing node is evaluated by our Trust Credit Assessment (TCA) scheme. Its represented by a collection of officiate history records denoted as H. Each requester node r holds her point of view regarding the trustworthiness of a inspector node i in the officiate history record which is managed by a trust management service. Each officiate history record is represented in a tuple that consists of the participatory sensing node primary identity P, the inspector node identity I, a set of trust credit T and the aggregated trust feedbacks weighted by the credibility Tc (i.e., $H = (P, I, T, Tc)$. Each credit in T is represented in numerical form with the range of [0, 1], where 0, +1, and 0.5 means negative feedback, positive

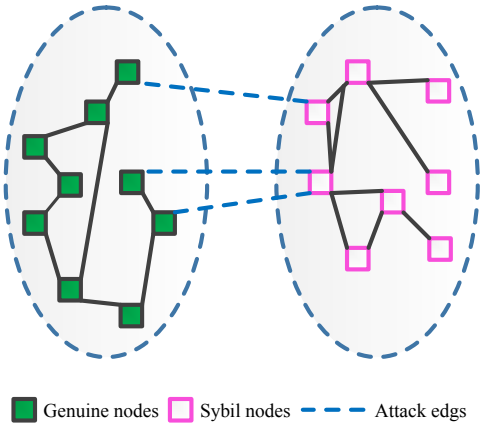

Fig. 4. A network topology diagram of suspicious Sybil attacks activities

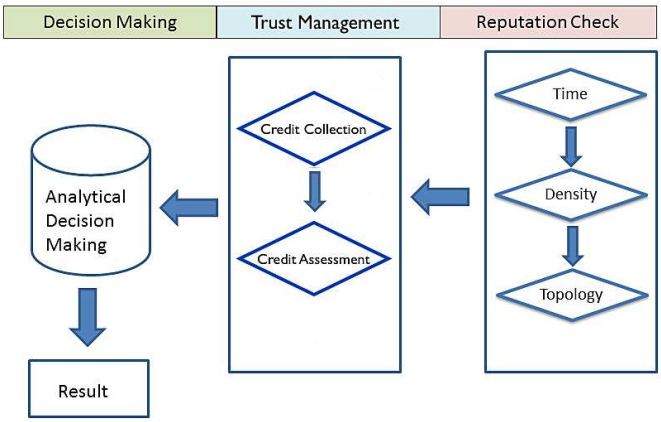

Fig. 5. Hybrid reputation monitoring diagram

feedback, and neutral respectively.

Whenever a requester node inquires the trust management service regarding the trustworthiness of a inspector node i, the trust result, denoted as $Tr(i)$, is calculated as the following:

$$Tr(i) = |v(i)|Tc(l,i)/|v(i)|, \tag{3}$$

where $V(i)$ is all of the feedbacks given to the inspector node i and $|V(i)|$ represents the length of the $V(i)$ (i.e., the total number of feedbacks given to the inspector node i). $Fc(l,i)$ are the trust feedbacks from the lth cloud consumer weighted by the credibility.

6) Analytical Decision Making: Base on both CCS and TCA examining result, each suspicious Sybil node will require an analytical decision making approaches to determine the probability. This problem is typically well suited to the application of structured decision processes. In a similar vein, analytical decisions are best approached by way of an analytical decision strategy. Observation credit result will be based on the investigation from the conditions described by CCS modules; therefore the results can not be generalized. Each decision described was assigned a score form with the range of [0, 1] , where 0, +1, and 0.5 means negative, positive, and neutral respectively. The credit result is presented as the percentage of threshold that similar to the pattern of Sybil attacks defined by author. The detection rate corresponds to the probability of detection Pd, whereas under normal conditions, it corresponds to the probability of declaring a false positive Fp. The detection rate and false-positive rate vary under different thresholds. In summarizing the results, if both CCS and TCA modules approached make a decision in a manner to be consistent with the defined threshold and score.

7) An Example of Scenario: As this attack has no relation to the identification scheme, we do not further evaluate it. On the other hand, an attacker can compromised and controlled by Sybil node. This compromised genuine node is considered as a Sybil node and not as an genuine node. This Sybil node will focus on create multiple online user identities called Sybil identities and try to achieve malicious results through these identities. As shown in Fig. 5, we will proceed in three phases. In the first phase, the server-side manager defined multiple adaptive thresholds including time, density and network topology to evaluate network trustworthiness. When multiple Sybil identities has been identified operation exceed adaptive threshold range in our CCS, CCS module will generate a notification to the TCA. Then TCA will officiate this inspector node history records from its database and process the credit accessment. Once the Sybil attacks pattern has been preliminary identified, it will enable Analytical Decision Making (ADM) to further analysis and determine the Sybil attacks in this network. This framework will check regularly network and system's statistics and use adaptive threshold to achieve network trustworthiness.

IV. Experimental Evaluations

In this section, the proposed algorithm Cloud based Trust Management Scheme (CbTMS) will be present and implement in OMNeT++ [14]. OMNeT++ is an extensible, modular, component-based, C++ simulation library and framework which also includes an integrated development and a graphical runtime. It provides a generic component architecture based on object oriented approach. Model components are termed modules which primarily communicate with each other via message passing either directly, or via pre-defined conditions and the message can arrive from another module or from the same module. We are currently implementing the CCS modules on each mobile participants as it well depicts a real world situation. This mobility model is based on entity mobility model where the nodes move independent of each other. We have taken following parameters for implementation as shown in Table I.

V. Conclusion

In this paper, we proposed a Cloud based Trust Management Scheme (CbTMS) framework for detecting Sybil attacks in participatory sensing network. Our CbTMS was proposed for performing trust management and reputation checker to verify coverage nodes in the participatory sensing. Sybil attacks focus

TABLE I
SIMULATION PARAMETER SETUP

Parameter	Values / Ranges
Simulation area	5000m × 5000m
Simulation time	1000s
Speed (m/s)	0.0 m/s to 5.0 m/s
Routing protocol	GPRS
Number of nodes (Max)	1000
Number of base stations	1-3
Traffic source	CBR
Pause time	Uniformly distributed in 0-50s
Packet size	256 bytes
Packet rate	5 packets/s
Transmission range	3000m

on creating multiple online user identities called Sybil identities and try to compromise system with its malicious results through these identities. This CbTMS framework combined two schemes namely Characteristics Checking Scheme (CCS) and Trust Credit Assessment (TCA) to a suspicious Sybil node observation. CCS was proposed for passively monitor suspected Sybil nodes characteristics including time, density and topology in the participatory sensing network simultaneously. TCA was proposed for evaluate trustworthiness of the suspected Sybil nodes. We are currently working on actual system testing to evaluate network performance in the detect of Sybil nodes based on OMNeT++.

ACKNOWLEDGMENTS

This work is supported in part by National Science Council, Taiwan, under contracts NSC 102-2218-E-011-001- and NSC 101-2622-E-152-003-CC3

REFERENCES

[1] J. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, and M. B. Srivastava, "Participatory sensing," in *Proc. ACM WSW*, Oct. 2006.

[2] T. Denning, A. Andrew, R. Chaudhri, C. Hartung, J. Lester, G. Borriello, and G. Duncan, "BALANCE: Towards a usable pervasive wellness application with accurate activity inference," in *Proc. ACM HotMobile 2009*, Feb. 2009.

[3] E. P. Stuntebeck, J. S. Davis, II, G. D. Abowd, and M. Blount, "HealthSense: Classification of health-related sensor data through user-assisted machine learning," in *Proc. ACM HotMobile 2008*, Feb. 2008.

[4] L. Deng and L. P. Cox, "LiveCompare: grocery bargain hunting through participatory sensing," in *Proc. ACM HotMobile 2009*, Feb. 2009.

[5] D. Mendez and M. A. Labrador, "On sensor data verification for participatory sensing systems," *Journal of Networks*, vol. 8, no. 3, pp. 576–587, Mar. 2013

[6] J. R Douceur, "The Sybil attack", in *Proc. IPTPS*, Mar. 2002, pp. 251-260.

[7] J. Grover, M. S. Gaur, and V. Laxmi, "A Sybil attack detection approach using neighboring vehicles in VANET," in *Proc. SIN 2011*, Nov. 2011, pp. 151–158.

[8] A. Josang and R. Ismail, "The Beta reputation system," in *Proc. 15th Bled Electron. Commerce Conf.*, Jun. 2002.

[9] S. Ries, "Extending Bayesian trust models regarding context-dependence and user friendly representation," in *Proc. ACM SAC 2009* Mar. 2009. pp. 213–237.

[10] I. Brandic, S. Dustdar, T. Anstett, D. Schumm, F. Leymann, and R. Konrad, "Compliant Cloud Computing (C3): Architecture and language support for user-driven compliance management in clouds," in *Proc. IEEE CLOUD 2010*, July 2010.

[11] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," *IEEE Internet Computing*, vol. 14, no. 5, pp. 14–22, Sep. 2010.

[12] C. Piro, C. Shields, and B. N. Levine., "Detecting the Sybil attack in ad hoc networks", in *SecureComm 2006*, Aug. 2006.

[13] S.-H. Chang and T.-S. Huang, "A fuzzy knowledge based fault tolerance algorithm in wireless sensor networks," in Proc. IEEE AINA 2012, Mar. 2012, pp.891–896.

[14] R. Hornig and A. Varga, "An overview of the OMNeT++ simulation environment," in *Proc. SIMUTools 2008*, 2008.